Exhibit 4

Excerpts of SW-SEC00013676

From: Quitugua, Eric [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=227693E84BC0400B84364660F692BC85-QUITUGUA, E]
Sent: 10/1/2018 10:14:56 PM
To: Starikevich, Stas [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=3d9f9e066cc7408db86a6930b1f5283f-Starikevich]
CC: Pitera, Wojciech [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=bfaa5564342d48259ec6c07248e40441-Pitera, Woj]; Brown, Timothy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1bcd95116e84d6692dd89f9d55c5b7a-Brown, Timo]
Subject: Re: OWASP SAMM Project
Attachments: SolarWinds Security Program Assessment - Sep 2018.xlsx

Thanks, I'll check it out.

Here is the excel file I showed during our meeting this AM.

solarwinds
Eric Quitugua | Information Security Manager
Office: 512.498.6200

From: Starikevich, Stas
Sent: Monday, October 1, 2018 2:26 PM
To: Quitugua, Eric
Cc: Pitera, Wojciech; Brown, Timothy
Subject: OWASP SAMM Project

Eric,

Here the OWASP SAMM (Software Assurance Maturity Model) we mentioned during the call:

https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Downloads

OWASP SAMM Project - OWASP

www.owasp.org

The foundation of the model is built upon the core business functions of software development with security practices tied to each (see diagram below).

Stas Starikevich, CISSP | Operations Engineer | SolarWinds MSP
Office: 984.227.6498

DOCUMENT PRODUCED IN NATIVE FORMAT

	Function	Category	CSC Top 20 Controls	Organization		
				CoreIT	MSP	Cloud
Cybersecurity Framework	Identify	Asset Management	1, 2	2	2	2
		Business Environment	-	3	3	2
		Risk Assessment	-	3	3	1
		Governance	4	3	3	1
		Risk Management Strategy	-	3	3	1
	Protect	Access Control	5, 9, 11, 12, 13, 14, 15, 16	2	2	2
		Awareness and Training	5, 17	1	1	1
		Data Security	1, 2	2	2	1
		Information Protection Processes and Procedures	3, 4, 7, 9, 10, 11, 18, 19	3	3	1
		Maintenance	3, 4, 5, 11, 12	3	3	0
		Protective Technology	5, 6, 7, 8, 11, 13, 14, 16	2	2	1
	Detect	Anomalies and Events	6, 9, 12, 19	3	3	1
		Security Continuous Monitoring	4, 8, 16, 19	3	2	0
		Detection Processes	19	3	3	0
	Respond	Response Planning	19	4	4	4
		Communications	19	4	4	4
		Analysis	6, 19	3	3	3
		Mitigation	4, 19	3	3	3
		Improvements	19, 20	3	3	3
	Recover	Recovery Planning	10	3	3	3
		Improvements	20	3	3	3
		Communications	-	4	4	4

Legend	
Maturity Level	Description
0	There is no evidence of the organization meeting the security control objectives or is unassessed.
1	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives
2	The organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
3	The organization has a documented, detailed approach to meeting the security control objectives, and regularly measures its compliance.
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.